

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of:

An Apple iPhone with Phone Number 254-630-3578. See Attachment A.

Case No. 19-M-125 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

An Apple iPhone with Phone Number 254-630-3578. See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

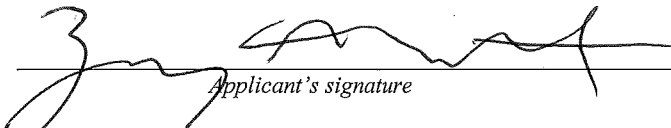
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1029(a)(2) (Trafficking in Unauthorized Access Devices), and 18 U.S.C. § 1028(a)(7) (Identity Theft).


The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Special Agent Zachary Hoalcraft, United States Secret Service
Printed Name and Title

Sworn to before me and signed in my presence:

Date: June 4, 2019


Judge's signature

City and State: Milwaukee, Wisconsin Case: 19-mj-00125-DEJ Filed: 06/13/19 Page: 1 of 15 Document: 1
Hon. David P. Jones, U.S. Magistrate Judge
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Zach Hoalcraft, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service and have been employed so since 2017. I am currently assigned to the U.S. Secret Service Milwaukee Financial Crimes Task Force (MFCTF). My duties include investigations into financial crimes, such as identity theft, check fraud, credit card fraud, bank fraud, wire fraud, currency-counterfeiting offenses, and money laundering. As a Task Force Agent, I have conducted investigations into wire fraud, money laundering, and other complex financial crimes. In the course of those investigations, I have used various investigative techniques, including undercover operations, reviewing physical and electronic evidence, and obtaining and reviewing financial records. In the course of these investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, and

ownership of proceeds of crime and to avoid detection by law enforcement of their underlying acts.

3. The information set forth herein is based on my training and experience, as well as information provided to me by witnesses and other members of law enforcement whom I believe to be reliable.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone with Phone Number 254-630-3578, hereinafter the "Device."

6. As discussed herein, the Device is believed to be the personal cell phone of DIANA GORDON.

7. The applied-for warrant would authorize the seizure and forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. Law enforcement has been conducting an investigation of ROBERT GORDON and DIANA GORDON for violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1028(a)(7) (identity theft), and 18 U.S.C. § 1029(a)(2) (access device fraud).

9. On May 28, 2019, U.S. Magistrate Judge David E. Jones of the Eastern District of Wisconsin issued a criminal complaint and arrest warrants for ROBERT GORDON and DIANA GORDON.

10. On May 28, 2019, U.S. Magistrate Judge Stephen L. Crocker of the Western District of Wisconsin issued a search warrant for residence of ROBERT GORDON and DIANA GORDON at 5815 Stella Avenue, Weston, Wisconsin, as well as three vehicles owned by ROBERT GORDON and DIANA GORDON. That search warrant authorized the seizure and search of records and information relating to violations of 18 U.S.C. §§ 1343, 1029(a)(2), and 1028(a)(7) occurring on or after June 1, 2018, including in any form located on electronic devices such as cell phones.

11. A copy of the Criminal Complaint and Application, as well as the Search Warrant and Application (herein "Residential Search Warrant), are attached hereto for the Court's review. The facts set forth in the Probable Cause sections of the Complaint Affidavit and the Residential Search Warrant Affidavit support probable cause for this requested warrant.

12. On May 30, 2019, agents executed the Residential Search Warrant and arrested ROBERT GORDON. However, at the time of the execution, it was learned that DIANA GORDON was presently out of state and intended to arrive back in Wisconsin on or around Sunday, June 2, 2019.

13. While law enforcement agents currently have the authority to track down DIANA GORDON, arrest her, and seize any electronic devices on her person pursuant to a lawful arrest, agents decided instead to contact DIANA GORDON, inform her of the arrest warrant, and permit her to turn herself in to the investigating agents when she returns to Wisconsin. Thus, on May 30, 2019, agents called DIANA GORDON at phone number 254-630-3578 (Device phone number), informed her of the arrest warrant, and she agreed to turn herself in to the investigating agents at the Milwaukee Federal Courthouse, 517 E. Wisconsin Avenue, Milwaukee, Wisconsin, 53202, at 10:00 a.m. on Thursday, June 6, 2019.

14. As set forth in the Criminal Complaint Affidavit and Residential Search Warrant Affidavit, and as further discussed herein, agents believe that DIANA GORDON'S cell phone contains evidence and fruits of the offenses at issue. Further, agents believe that DIANA GORDON'S cell phone is an Apple iPhone with Phone Number 254-630-3578 (the Device).

15. For instance, records from Kohl's show 10 orders placed on 11/19/2018, 11/28/2018, 12/02/2018, 01/12/2019, 01/23/2019, 02/04/2019, 03/10/2019, through the account of DIANA GORDON, which has a listed phone number of 254-630-3578

(Device phone number). Kohl's records show that all of these orders were placed through an iPhone device. For all but one of these orders, DIANA GORDON used Kohl's Cash certificates issued in the names of other people. These orders include online order #xx0558 (December 2, 2018), online order #xx1133 (January 12, 2019), and online order #xx2972 (February 2, 2019) referenced at paragraphs 30(b), 30(d), and 30(g) in the attached Residential Search Warrant Affidavit (and paragraphs 27(b), 27(d), and 27(g) of the Complaint Affidavit). As noted in that Residential Search Warrant Affidavit and Complaint Affidavit, each of those orders included use of Kohl's Cash certificate information issued to another person who later complained to Kohl's.

16. Further, on May 30, 2019, seized and briefly reviewed ROBERT GORDON's cell phone during execution of the warrants. Among other things, agents observed recent text messages to and from the Device phone number, 254-630-3578, in which Robert Gordon texted Kohl's Cash certificate information to that number.

17. While law enforcement officers may already have the authority to seize and search the Device under the criminal complaint, arrest warrant, and Residential Search Warrant, I seek this additional warrant out of an abundance of caution to be certain that the seizure and examination of the Device in the Eastern District of Wisconsin will comply with the Fourth Amendment and other applicable laws.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Apple Devices:* As described in Attachment A, the Subject Device is an Apple brand device. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

a. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

b. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used

instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

c. The passcode or password that would unlock the Device is not known to law enforcement. Thus, it will likely be necessary to press the finger of the user of the Device to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device via Touch ID with the use of the fingerprints of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

22. As discussed above, the Device is believed to be the personal cell phone of DIANA GORDON. Thus, it is anticipated that her fingerprints are among those that would be able to unlock the device via Touch ID.

23. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Subject Device as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

24. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of DIANA GORDON to the Touch ID sensor of the Device for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched is an Apple iPhone with Phone Number 254-630-3578, hereinafter the "Device."

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records relating to violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1029(a)(2) (Trafficking in Unauthorized Access Devices), and 18 U.S.C. § 1028(a)(7) (Identity Theft), those violations involving Robert Gordon or Diana Gordon, and occurring after June 1, 2018, including:

- a. Records and information relating to Kohl's, including Kohl's merchandise, cash, certificates, coupons, and accounts;
- b. Records and information relating to @OfficialJigLord or other online accounts;
- c. Records and information relating to businesses' customer account information and rewards program information, including usernames, passwords, points, certificates, coupons, codes, and related items;
- d. Records and information relating to selling, purchasing, or advertising of goods or services;
- e. Records and information relating to the identity or location of the Robert Gordon and Diana Gordon and accomplices involved in obtaining, transferring, selling, and buying usernames, passwords, Kohl's Cash certificates, and other business rewards program items.
- f. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe

deposit box and records, financial records or notes showing payment, receipt, concealment, transfer, or movement of money generated from or connected to the sales of Kohl's cash and related business loyalty rewards items, or financial transactions related to such activities, including any virtual or crypto currency.

g. Records and information relating to obtaining, maintaining, transferring, or spending money or other things of value;

h. Records and information relating to accessing or using personal identifying information, including email addresses, usernames, codes, user IDs, PIN numbers, and passwords.

i. Records of off-site storage locations, and records and receipts and rental agreements for storage facilities;

j. Records and information relating to unlawful or surreptitious access to information;

k. Records and information relating to communications between Robert Gordon and Diana Gordon, as well as records and information relating to communications between Robert Gordon or Diana Gordon relating to the offense(s), including sales, advertising, customers, potential customers, payments, credit, currency, means of identification, or access devices;

l. Records and information relating to preparatory steps taken in furtherance of the offense(s);

m. Records and information relating to efforts prevent detection of the offense(s);

n. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored.

During the execution of the search of the Device described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Diana Gordon to the Touch ID sensor of the Device, if applicable, for the purpose of attempting to unlock the Device via Touch ID in order to search the contents as authorized by this warrant.